AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Anthony Safford, being first duly sworn, hereby depose and state as follows:

INTRODUCATION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Department of Homeland Security, Homeland Security Investigations (HSI), and have been so employed since January of 2023. As part of my duties as an HSI SA, I investigate criminal violations relating to child exploitation including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, 2251A, 2252A, and 2260, the sexual abuse of children in violation of 18 U.S.C. §§ 2422 and 2243, and the sex trafficking of children in violation of 18 U.S.C. § 1591. I have received training in child pornography and child exploitation investigations and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in different forms of media including computer media. Prior to my appointment as a SA with HSI, I was employed as a Special Agent with the Internal Revenue Service, Criminal Investigation (IRS CI) for one year, where it was my duty to investigate tax fraud, money laundering and public corruption. Before becoming an SA with IRS CI, I was a Deportation Officer with Immigration and Customs Enforcement, Enforcement and Removal Operations for two years. As a Deportation Officer, it was my job to enforce the criminal and administrative provisions of Title 8 of the United States Code and Title 18 of the United States Code as they relate to immigration. I have conducted and participated in a wide array of criminal investigations. In addition to my investigative experience, I have received over 2,000 hours of investigative and law enforcement training from the Federal Law Enforcement Training Center. My investigative experience detailed herein, as well as my training, and the investigative experience of other officers who have participated in this investigation, serve as the basis for the

conclusions set forth herein. I am a law enforcement officer of the United States, within the meaning of Section 115(c)(1) of Title 18 of the United States Code, who is "authorized by law or by government agency to engage in or supervise the prevention, detection, investigation or prosecution of any violation of Federal Criminal Law." Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2252. I am an "investigative or law enforcement officer" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

2. This affidavit is being submitted for the limited purpose of establishing probable cause to believe that Seth Jacob SCHWERIN, date of birth XX/XX/1993 (hereinafter SCHWERIN), has committed violations of 18 U.S.C. §§ 2252(a)(1), transportation of a visual depiction of a minor engaged in sexually explicit conduct; 2252(a)(2), receipt and distribution of visual depictions of minors engaged in sexually explicit conduct; and 2252(a)(4)(B), possession of visual depictions of minors engaged in sexually explicit conduct.

3. The statements contained in this affidavit are based upon my personal knowledge and observations, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records. This affidavit includes only those facts that I believe are necessary to establish probable cause and does not include all the facts uncovered during the investigation.

RELEVANT STATUTES

4. There is probable cause to believe that SCHWERIN committed violations of the following statutes:

a. 18 U.S.C. § 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer or mail, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. 18 U.S.C. § 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any

means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

DEFINITIONS

5. The following definitions apply to this Affidavit and its Attachments:

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "sexually explicit conduct," used generally, 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. For the purposes of this affidavit, "Child Sexual Abuse Material," abbreviated as CSAM, means any material in any form at which depicts a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A)(i-v). CSAM has the same meaning as the term "child pornography."

d. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted

by any means, whether or not stored in a permanent format.

e. The term "computer," as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

f. A "wireless telephone" (or mobile telephone, or cellular telephone, or just cell phone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the

Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e- mail, remote storage, and co-location of computers and other communications equipment.

h. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers and/or letters separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. A creation IP address is the address used on the date that an e-mail or other account is created by the user.

i. The "International Mobile Equipment Identity" or IMEI is a 15-17-digit number that is given to every mobile phone. This number is used by service providers to uniquely identify valid devices. The IMEI can provide information about the country and network from which a device originated, the warranty, carrier information, and more similar details.

j. The "International Mobile Subscriber Identity" (IMSI) is a unique number up to 15 digits which is assigned to a subscriber on a mobile network. Mobile

network operators use IMSI to identify a subscriber's country, mobile network, and phone number, among other things.

BACKGROUND ON KIK

6. Kik is a free service that is downloaded from the Internet. Kik Messenger (hereinafter "Kik") advertises itself as "the first smartphone messenger with a built-in browser." Kik allows users to talk to their friends, browse and share any web site with a Kik user's friends. According to the website, Kik offers a simple, fast, most life-like chat experience you can get on a smartphone. Unlike other messengers, Kik usernames - not phone numbers - are the basis for Kik user accounts, so Kik users are in complete control with whom they communicate. In addition, Kik features include more than instant messaging. Kik users can exchange images, videos, sketches, stickers and even more with mobile web pages.

7. The Kik app is available for download via the App Store for most iOS devices such as iPhones and iPads. Additionally, the Kik app is available on the Google Play Store for Android devices. Kik can be used on multiple mobile devices, to include cellular phones and tablets.

8. In general, providers like Kik ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address.

9. Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of

the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

10. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems or complaints from other users. Providers typically retain records about such communications, including records of e-mails and other contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

11. As explained below, information stored at MediaLab.ai Inc., parent company of KIK, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation. In my training and experience, the data pertaining to an account that is retained by a provider like Kik can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up- and other communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a Kik account at a relevant time. Further, such stored electronic data can show how and when the account was accessed or used. Such "timeline" information allows investigators to understand the chronological context of the usage of an account, account access, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the user of a Kik account. Additionally, stored electronic data may provide relevant insight into the

state of mind of the user of a phone number as it relates to the offense under investigation. For example, information relating to a particular Kik account may indicate the user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

12. Kik offers users the ability to create an identity within the app referred to as an "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to obtain a different username. The username for a particular Kik account holder is generally displayed in their Kik profile.

13. In October 2019, Kik, formerly headquartered in Canada, was purchased by MediaLab.ai Inc., a company operating in the United States in California.

Information Regarding NCMEC

14. The National Center for Missing and Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further their mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the Cyber Tipline and Child Victim Identification Programs. NCMEC makes information submitted to the Cyber Tipline and Child Victim Identification Programs available to law enforcement and uses this information to help identify trends and create child safety and prevention messages. As a national clearinghouse, NCMEC also works with Electronic Service Providers (ESPs), law enforcement, and the public in a combined effort to reduce online child sexual abuse material.

15. Companies that suspect child pornography has been stored or transmitted on their systems report that information to NCMEC in a CyberTipline Report (or "CyberTip"). The ESP submits the report and uploads content to NCMEC via a secure connection, which in turn, assists NCMEC in trying to identify the victims depicted. Using publicly available search tools, NCMEC then attempts to geo-locate where the activity occurred based on the information the ESP submits, such as IP addresses. NCMEC then packages the information from the ESP along with any additional information it has, such as previous related CyberTips, and sends it to law enforcement in the jurisdiction where the activity is believed to have occurred.

INVESTIGATION AND PROBABLE CAUSE

Undercover Communications

16. On December 2, 2024, an HSI Detroit undercover agent (UCA) was conducting an undercover chat investigation on Kik. The UCA was portraying himself as the father of an 8-year-old girl. As part of this investigation, the UCA was part of a publicly available chat group on KIK with a chat group name indicative of incest.[1]

17. While in the KIK chat group, Kik user **fundaddd08**, also referred to herein as TARGET ACCOUNT 1, asked the group if anyone was in Ohio. TARGET ACCOUNT 1 later sent another message asking, "Anyone else in Ohio or nearby? Wanna hang out? Daughter is 8 here."

18. The UCA also observed another message from a different Kik user which was an invitation for a private chat group. The UCA joined this group and again noticed that TARGET

[1] The names of chat groups are known but not disclosed herein.

ACCOUNT 1 was also a member of this private chat room. While in that private chat room, the UCA reported that other users were posting images and videos of suspected and obvious child sexual abuse material (CSAM) or child pornography. Between December 3-5, 2024, the UCA reported seeing several images and videos posted by TARGET ACCOUNT 1. Specifically, one image showed a prepubescent girl, approximately 5-8 years old, wearing long socks, leaning back on the floor, with her vagina and anus exposed. TARGET ACCOUNT 1 also uploaded a 29-second video of a young prepubescent girl approximately 8-12 years old, naked form the waist down and masturbating with her fingers.

19. The UCA was also a member of another Kik chat group and again noted that TARGET ACCOUNT 1 was also a member. The UCA reported that TARGET ACCOUNT 1 posted an image that depicts an approximately 7-10-year-old girl, naked, holding a bottle of clear liquid, and her vagina exposed.

20. [redacted]

[redacted]

21. On December 4, 2024, HSI Detroit sent KIK a summons for subscriber info related to TARGET ACCOUNT 1, "fundaddd08." On December 7, 2024, Kik responded to the summons with the following information:

Date: December 7, 2024
First Name: fundaddd08
Last Name: (blank)
Registration Email: **schwerinseth@gmail.com** (unconfirmed)
Username: fundaddd08
IP address: **69.133.3.232**

22. On December 9, 2024, HSI Detroit sent a summons to Internet Service Provider (ISP), Charter Communications Inc., for subscriber information related to IP address **69.133.3.232** for December 2, 2024, at 9:26 Greenwich Meant Time (GMT) (also known as Zulu time or coordinated universal time (UTC)). On December 12, 2024, Charter Communications responded and provided the following information:

Subscriber Name: **Seth SCHWERIN**

Service Address: 7 Summerplace Drive, Wapakoneta, OH 45895-1834

User Name or Features: 5675251828@charter.net, S.J.Schwerin04@gmail.com, and **Schwerinseth@gmail.com**

Start Date: 09/15/2024 at 04:26 PM

End Date: 12/10/2024 at 10:07 AM

Cyber Tipline Reports

23. On December 13, 2024, MediaLab, aka Kik, submitted Cyber Tipline Report (CT) 203508826 to the National Center for Missing and Exploited Children (NCMEC), reporting that 38 files of CSAM had been uploaded to Kik between December 3, and December 12, 2024, by TARGET ACCOUNT 1, **fundaddd08**. Kik indicated that each file was sent by TARGET CCOUNT 1 to another user in a private chat or to other users in a group chat. Kik reported that the home email address on the Kik user was **schwerinseth@gmail.com**. Multiple IP addresses were used, including IP address **69.133.3.232** which was associated to three CSAM files uploads. This was the same IP address used to distribute the child pornography to the UCA in this case and that came back to Seth SCHWERIN at his residence. Affiant viewed 33 files[2] of suspected CSAM; 24 of the files depict a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A). A description of one of the files is as follows:

a. Ed2f534e8214be1c38d321d1c1897602

This file is a 26-second video depicting a prepubescent minor, naked from the waist down and lying on her back with her legs spread, exposing her vagina. An adult male presses and rubs his erect penis against the minor's naked vagina and eventually ejaculates over her vagina. At one point, the camera pans over the minor's face and full body.

[2] Only 33 from CT 203508826 were available to Affiant. Some of the files may be duplicates that were distributed to different users or groups on KIK.

24. On January 3, 2025, while conducting database research and open-source intelligence research, a program which queries previously filed NCMEC CTs was utilized. When the IP address **69.133.3.232** was used as the search term, another CT was located. On November 1, 2024, NCMEC received CT 201849837 from Kik which alleged that the user **taste.ur.vag,** hereinafter TARGET ACCOUNT 2, uploaded five files of CSAM. The CT indicated that the files were sent from TARGET ACCOUNT 2 to another user via private message. Affiant viewed three[3] files of suspected CSAM; two of the files depict a minor engaged in sexually explicit conduct. A description of one of the files is as follows:

a. 93002a8a45b3cfbb4cef99de7011864f

A video file 11 seconds in duration. The video file depicts a minor who is naked from the waist down and her vagina is completely visible. The minor has narrow hips, no pubic hair, shaved or otherwise, and a high-pitched voice. In the video the minor is lying on her back and an adult male inserts his erect penis into her vagina and engages in intercourse until the minor pulls away.

25. On January 3, 2025, an analyst from the Ohio Internet Crimes Against Children Task Force (ICAC) sent Charter communications an exigent request for the subscriber information for two of the IP addresses from CT 201849837: 69.133.3.232: port 59196 on October 27, 2024, at 23:43:48 universal coordinate time (UTC), and 69.133.3.232: port 61636 on October 31, 2024, at 18:31:38 UTC. Similarly to the summons that HSI Detroit sent to Charter Communications for

[3] Only 3 files from CT 201849837 were available to your Affiant.

the IP addresses from the undercover communications with TARGET ACCOUNT 1, the responsive information, which was received that same day, listed the subscriber as Seth SCHWERIN, 7 Summerplace Drive, Wapakoneta, Ohio 45895.

26. Many of the IP addresses from the two CTs from Kik belonged to Verizon Wireless. On January 3, 2025, the same analyst from ICAC sent Verizon Wireless an exigent request for one of the Verizon Wireless IP addresses, but Verizon indicated that it was unable to determine a specific user because the IP addresses were part of a Network Address Translation (NAT), which allows multiple devices to be connected to one public IP address, common for devices connected to a cellular network, such as a cell phone.

27. A database housing Ohio driver's license records was queried and SCHWERIN's driver's license record was located. The driver's license record included the following information: name: Seth Jacob SCHWERIN; date of birth: XX/XX/1993; and social security number: XXX-XX-1861. The address listed was 7 Summerplace Drive, Wapakoneta, Ohio 45895, the same address listed on the records from Charter Communications for the subscriber of the IP address **69.133.3.232.**

Search Warrant of 7 Summmerplace Drive

28. On the evening of January 3, 2025, members of HSI Cleveland, ICAC, the Ohio Bureau of Criminal Investigation, Wapakoneta Police Department, and the Auglaize County Sheriff's Office executed a residential search warrant at 7 Summerplace Drive, Ohio, 45895. Law enforcement encountered SCHWERIN, SCHWERIN's significant other, and three minor children at the residence.

29. During the search warrant, SCHWERIN was interviewed and admitted that he lived at the residence, his phone number was **419-231-2471**, hereinafter the SUBJECT PHONE, and his

email was schwerinseth@gmail.com, the same email in the CyberTip involving Kik user **fundaddd08**. SCHWERIN said he worked as a semi-truck driver for Buschur Custom Farms. SCHWERIN's trips are mostly day trips, that is, he departs and returns home in the same day, but he occasionally has overnight trips where he will spend at least one night away from home in transit. SCHWERIN denied knowledge of the KIK TARGET ACCOUNTS 1 and 2 and denied child pornography activity. He did, however, admit in that interview that he had once had a Kik account, although he claimed it was several years prior. It should be noted that in his subsequent polygraph interview that day, SCHWERIN then admitted that he had in fact, downloaded Kik more recently (two months earlier) but claimed he deleted it the same day without logging on or creating a new Kik account. [redacted]

30. During the search, electronic devices were discovered, triaged and searched on site. None of the electronic devices searched on site were found to have CSAM. Some of the electronic devices, to include an Apple iPhone 15 Pro Max, were seized pursuant to the warrant.

Search Warrants for KIK Accounts

31. On January 3, 2025, the Honorable United State Magistrate Judge Darrell A. Clay of the Northern District of Ohio signed and issued a federal search warrant (*see* 25mj5005) for the contents and communications of the KIK accounts **fundaddd08**, TARGET ACCOUNT 1, and **taste.ur.vag.**, TARGET ACCOUNT 2. MediaLab.ai/KIK was served the search warrant on January 4, 2025, and produced the requested records and information that same day.

32. The records from Kik included approximately 129 media files which Affiant viewed. Of those, 26 files, 24 from **fundaddd08** and 2 from **taste.ur.vag.**, depict a minor engaged in sexually explicit conduct. A description of one of those files is as follows:

a. 8019a198-5ec9-4053-9f08-83a73c0fad

A video file one minute and 36 seconds in duration. The video depicts a prepubescent minor female, naked, with her vagina and anus exposed to the camera. The minor is posed on her knees and elbows facing away from the camera and her backside is facing the camera. During parts of the video, you can see her face through the gap in her legs. During the video, an adult female performs oral sex on the minor's vagina and penetrates and stimulates the minor's vagina with a sex toy.

33. Numerous images and videos contained in the CTs are also contained in the Kik records responsive to the search warrant. The media files from both TARGET ACCOUNT 1 and TARGET ACCOUNT 2 included images of SCHWERIN.

34. The Kik contents responsive to the search warrant included the chat message communications sent and received by TARGET ACCOUNTS 1 and 2. The messages reviewed are consistent with the production, distribution and receipt of material depicting minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A). The chats reveal that the user of the target accounts has a father-daughter sexual fantasy and is interested in other individuals with daughters. Some excerpts of the chats are contained below:

a. [redacted]

[redacted]

b. [redacted]

c. [redacted]

[redacted]

d. [redacted]

[4] Files received by the target accounts were not included in the KIK records, only those which were sent by the target accounts.

e. [redacted]

35. The Kik contents responsive to the search warrant included logs which show the files distributed by TARGET ACCOUNTS 1 and 2, the Kik user those accounts distributed the file to, the IP address used to distribute the file, and the date and time the file was sent. The Kik logs show that approximately 77 of the 83 files distributed from specifically TARGET ACCOUNT 1 were distributed using Verizon Wireless IP addresses. The 3 files of CSAM distributed from TARGET ACCOUNT 2 were distributed from Verizon Wireless IP addresses.

36. SCHWERIN's employer, Buschur Custom Farms, provided law enforcement with SCHWERIN's work schedule. SCHWERIN's work schedule showed the days he worked or drove on work trips. Affiant reviewed those records and cross-referenced them to the Kik records/logs and the two CyberTipline Reports.

37. Every time TARGET ACCOUNT 1 distributed a media file (whether CSAM or not), it coincided with a day SCHWERIN was scheduled to drive on a work trip. Every time TARGET ACCOUNT 2 distributed a file depicting specifically CSAM, it coincided with a day SCHWERIN was scheduled to work/drive on a work trip.

38. The aforementioned Kik logs detail the file, receiver, IP address, and date and time it was sent but do not include the port that a device used to connect to an IP address. Verizon Wireless requires a port number to determine which user, or in this case which cell phone number, used the IP address in question due to the IP address using the NAT to allow multiple phone numbers to utilize one IP address. The Kik records include the chat messages that the TARGET ACCOUNTS sent. The records detailing those chat messages list the IP address and port number associated with each message sent. Affiant was able to locate messages close in time to 11 CSAM files which were sent by the TARGET ACCOUNTS, as well as messages close in time to IMAGE B.[5]

39. On January 8, 2025, Affiant sent a subpoena to Verizon Wireless for the cell phone number and subscriber information associated with 16 IP addresses and port numbers. That same day, Verizon Wireless provided the requested records. All 16 IP addresses come back to **419-231-2471**, the phone number SCHWERIN admitted was his (hereinafter referred to as the SUBJECT PHONE). The records list device information to include the International Mobile Equipment Identity (IMEI): **354068588595420**, and the International Mobile Subscriber Identity (IMSI):

---

[5] IMAGE B is described in paragraph 20 and was one of the images that the KIK TARGET ACCOUNT 1 user distributed to the UCA in this investigation. IMAGE B depicts an adult male pressing his erect penis against the naked vagina of a prepubescent minor.

311480101752535. The records further indicate that the phone number was activated on the Verizon Wireless network on August 24, 2024. The subscriber was listed as Sheryl Schwerin, later determined to be SCHWERIN's mother, at an address in Huntsville, Ohio.

40. Affiant later discovered that the port numbers for every file of CSAM uploaded or distributed by TARGET ACCOUNT 1 and 2 were included in the Cyber Tipline Reports (CT). The records from Verizon did not include a single point in time and a single port number but rather showed the entire timeframe the SUBJECT PHONE used a particular IP address, and the entire range of port numbers used during that timeframe. For instance, one of the IP addresses and dates and times Affiant subpoenaed Verizon for was 174.196.96.179 and port 62821 on October 25, 2024 at 15:21:04 UTC. While the Verizon records did not just show which phone number used that IP address on that exact queried date and time, they showed that the SUBJECT PHONE used that IP address from October 24, 2024, 16:52 UTC, to October 29, 2024, 13:07 UTC, and used port numbers 62816 to 62847 during that period.

Computer Forensics

41. Forensic analysis of the Apple iPhone 15 Pro Max belonging to SCHWERIN and that was seized during execution of the residential search warrant revealed the following:

a. The phone number assigned to SCHWERIN's phone is **419-231-2471,** the SUBJECT PHONE**.**

b. The IMEI is **354068588595420**, the same IMEI from the Verizon Wireless records responsive to a subpoena querying the IP addresses from the Kik activity. There were three IMSIs listed, including **311480101752535**, which was also present in the Verizon Wireless records.

c. There were numerous images of SCHWERIN's face, as well as a picture of his driver's license. One cached image file found on the phone depicts an approximately 10-12-year-old minor performing oral sex on an adult penis.

d. The following are just some of the search terms found on SCHWERIN's phone:

   i. "daughter gives dad a blowjob"

   ii. "daughter giving blowjob"

   iii. "daughter sucking dads big dick"

   iv. "step daughter blowjob"

   v. "mom.gives son a blowjob" [sic]

   vi. "daughter sucking off dad"

e. The forensic examiner did not locate the Kik app on the phone but did locate Kik artifacts proving that it had been downloaded to the phone at some point and that TARGET ACCOUNT 1 had been used on the phone. In SCHWERIN's Apple Keychain,[6] he had the Kik account **fundaddd08,** TARGET ACCOUNT 1, which was created on December 2, 2024. The email account on the phone was **schwerinseth@gmail.com**. The forensic examiner also found an email from Kik dated December 2, 2024 that said, "Welcome to Kik!" and, "Your username is: **fundaddd08**." It should be noted that the Kik child pornography activity reported in CyberTipline Report 203508826 occurred on various dates

[6] Apple Keychain is a phone application on Apple devices that stores usernames and passwords to the user's various accounts.

beginning on that very same date (December 2, 2024) and continued until December 12, 2024.

42. Forensic analysis of the phone revealed GPS coordinates for various dates and times.

Summons to Google

43. On January 13, 2025, Google was summonsed for the subscriber and IP address information for Google account, schwerinseth@gmail.com (the email used to sign up for TARGET ACCOUNT 1 and same email on SCHWERIN's phone), and s.j.schwerin04@gmail.com (the email used for SCHWERIN's Apple account on his Apple iPhone 15 Pro Max). On January 20, 2025, Google provided the requested records.

44. The subscriber information for **schwerinseth@gmail.com** was:

name: **Seth Schwerin**
phone: **419-231-2471**
recovery email address: **s.j.schwerin04@gmail.com**.

45. The subscriber information for s.j.schwerin04@gmail.com was:

name: **Seth Schwerin**
phone: 812-621-6796

GPS Data from Employer

46. On January 15, 2025, Affiant interviewed SCHWERIN's employer, David Buschur, the President of Buschur Custom Farms which provides farms with logistical and transportation services. SCHWERIN was employed as a truck driver and usually transported livestock between farms, or farm waste to dump sites. Most of SCHWERIN's trips were day trips

where he left home and returned home in the same day, although he occasionally drove on overnight trips where he spent at least one night away from home.

47. Buschur advised that his company used a program that allowed him to track his semi-trucks using Global Positioning System (GPS) data. This program allows Buschur to view in live time where his trucks are and to view historical data of where his trucks have been. Buschur advised that he maintained a detailed list of his employees' schedules, including SCHWERIN's work schedule from the time he began working for him, as well as the GPS data for every trip SCHWERIN went on, thus, enabling him to account for SCHWERIN's whereabouts whenever he was driving one of Buschur's trucks.

48. Buschur provided SCHWERIN's location for the date and time of each CSAM upload from the two KIK TARGET ACCOUNTS.

Summons to Charter Communications

49. On January 21, 2025, Charter Communications was served a summons for the subscriber information for an IP address associated with activity from the Kik target accounts, and more specifically, uploads of at least two files of CSAM and IP address **69.133.3.232,** and three different dates/times. On January 24, 2025, Charter Communications produced the requested records. That IP address and the queried dates and times all came back to Seth SCHWERIN at 7 Summerplace Dr, Wapakoneta, OH 45895. The subscriber information contained three email addresses, two of which were s.j.schwerin04@gmail.com, the email used for SCHWERIN's Apple account on his Apple iPhone, and **schwerinseth@gmail.com**, the email used to sign up for KIK TARGET ACCOUNT 1. The phone number on the account was 567-525-1828, which belonged to SCHWERIN's live-in girlfriend. The MAC address was C03C049D3930, the same MAC

address found on the router inside SCHWERIN's home during the execution of the residential search warrant.

Review of Data and Records

50. After reviewing the Kik records/data, the IP records from Verizon, the IP information from Charter Communications, the cached GPS data on SCHWERIN's cell phone, and the GPS data provided by SCHWERIN's employer, David Buschur, Affiant was able to confirm that there were 12 CSAM files distributed by KIK TARGET ACCOUNT 1, **fundaddd08**, and one file of CSAM distributed by TARGET ACCOUNT 2, **taste.ur.vag.**, in the Northern District of Ohio (i.e., when the file upload occurred). They are listed below.

a. On December 3, 2024, TARGET ACCOUNT 1, between 17:16-17:22 UTC, distributed ***four*** files to a group chat with multiple other users—two at 17:16 UTC, one at 17:18 UTC, and one at 17:22 UTC, but they are grouped here because they were sent using the same IP address and port. Thy were uploaded using Verizon IP 174.196.123.76, port 3699, and Verizon records show that SCHWERIN's phone number **419-231-2471** used Verizon IP 174.196.123.76, ports 3680-3711, on December 3, 2024, from 10:17-20:40 UTC. Thus, these files were uploaded from TARGET ACCOUNT 1 on a phone assigned SCHWERIN's phone number. Cached on the phone was GPS coordinates for the date and times of the file uploads, all of which came back in this District. While he worked that day and was driving truck 35, Buschur's GPS data shows that truck 35 was at 402 Leon Pratt Drive, Wapakoneta, OH, at 17:16, 17:18 and 17:22 UTC, and thus, in this District at the time of the uploads.

b. On December 3, 2024, at 17:45 UTC, TARGET ACCOUNT 1, **fundaddd08**, distributed CSAM to another user—file name: 40f76ca8-4bf4-43b0-b132-0b71ce079e43, referred to earlier as IMAGE B, depicting a prepubescent minor, naked from the waist down, lying on her back with an adult erect penis pressed against her vagina. This image was uploaded from TARGET ACCOUNT 1 using Verizon IP 174.196.123.76. While the port was not available in the KIK records or CyberTips, the IP addresses from the messages preceding and following the file upload were the same and had port number 3699. Verizon records reveal that **419-231-2471**, SCHWERIN's phone number, used that IP (174.196.123.76), ports 3680-3711, on December 3, 2024 from 10:17-20:40 UTC, to upload this file. Located on SCHWERIN's phone were GPS coordinates corresponding with the upload date and time and that prove the file was uploaded in the Northern District of Ohio. SCHWERIN's work schedule, as provided by Buschur, showed that he worked on December 3, 2024, and was in truck 35. On December 3, 2024, at 17:45 UTC, truck 35 was at US-33, Wapakoneta, Ohio 45895, in the Northern District of Ohio.

c. On December 3, 2024, at 20:25 UTC, KIK TARGET ACCOUNT 1 distributed to another user CSAM file 8019a198-5ec9-4053-9f08-83a73c0fad57, a one-minute-36-second video depicting a naked prepubescent minor on her elbows and knees facing away from the camera with her vagina and anus facing the camera. In the video, an adult female performs oral sex on the minor and stimulates and penetrates the minor with a sex toy. This image was uploaded from TARGET ACCOUNT 1 using Charter IP 69.133.3.232, port 53462. Charter records indicate that the subscriber and address for that IP and port number at the upload date/time is Seth SCHWERIN at his

residence (7 Summerplace Drive, Wapakoneta, OH 45895)—i.e., this file was distributed via the wireless internet at SCHWERIN's residence. While his work records show he was working that day, they also show the Buschur truck he was driving parked at 402 Leon Pratt Drive, Wapakoneta, OH 45895, just a six-minute drive from his residence, for approximately one hour and 21 minutes from 20:00-21:22 UTC. Further, the GPS data from SCHWERIN's phone itself proves that at approximately 20:25 UTC, his phone was at his Wapakoneta residence.

d. On December 3, 2024, at 20:34 UTC, TARGET ACCOUNT 1 distributed to another user CSAM file 7e56940b-9841-4149-a2c5-cecaea9c0258, a 37-second video depicting a naked prepubescent minor with her face, breasts and vagina visible. In the video the minor female is sitting on the ground facing the camera with her legs spread. The minor female digitally stimulates and penetrates her vagina. This file was uploaded using Charter IP 69.133.3.232, port 53527. Charter records indicate that the subscriber and address for that IP address and port number at the upload date/time is Seth SCHWERIN at his Wapakoneta residence. Thus, this was distributed using the wireless internet at SCHWERIN's residence and while work records show SCHWERIN was working that day, they also show that his truck that day was at 402 Leon Pratt Drive, Wapakoneta, OH 45895 for approximately one hour and 21 minutes from 20:00 UTC to 21:22 UTC. Further, the cached GPS data from his cell phone shows that at 20:33 UTC (a minute before the file upload time), his phone was at GPS coordinates coming back to his nearby Wapakoneta residence.

e. On December 3, 2024, at 21:16 UTC, TARGET ACCOUNT 1 sent another user CSAM file bbfa4d84-7144-491b-a38e-cc320ef25db0, a one-minute video depicting

a naked prepubescent minor's face, breasts, vagina and anus visible, lying on what appears to be a bed with her legs spread, while she digitally stimulates and penetrates her vagina. This image was uploaded using Verizon IP 174.196.123.76, port 3752. Verizon records show that SCHWERIN's phone number **419-231-2471** used the IP 174.196.123.76, ports 3744-3775, on December 3, 2024 from 10:20-23:35 UTC, meaning that this file of CSAM was uploaded from TARGET ACCOUNT 1 on a phone assigned SCHWERIN's phone number. Cached on the phone was a GPS coordinate for the date and time of the file upload that came back to the corner of Dixie Highway and Short Road in Wapakoneta, OH. This file was also uploaded during the time his Buschur truck was parked at 402 Leon Pratt Drive, Wapakoneta, OH (20:00-21:22 UTC), and GPS data from his phone places his phone approximately 0.7 miles from the truck at 21:16 UTC and thus, in this District.

f. On December 5, 2024, at 10:01 UTC, TARGET ACCOUNT 1 distributed ***two*** CSAM files using the same IP and port: (1) image file 023de793-3f3a-4a0e-aea1-8d156a3eec3a, depicting a prepubescent minor, naked, her face visible, sitting on a bed with her legs spread, and (2) image file 023de793-3f3a-4a0e-aea1-8d156a3eec3a, depicting two prepubescent minors, naked, sitting on what appears to be a blanket with their hands propping them up and their legs outstretched in front of them, lasciviously displaying their vaginas. These were distributed using Verizon IP 174.219.212.255, port 2502, and Verizon records show that SCHWERIN's phone number **419-231-2471**, used that IP, ports 2496-2527, from December 4, 2024, 05:42 UTC to December 6, 2024, 05:46 UTC, consistent with these files being uploaded from TARGET ACCOUNT 1 on a phone with SCHWERIN's **419-231-2471** number.

The cached GPS coordinates on his phone demonstrate that these files were uploaded in this District. While Buschur records show SCHWERIN worked that day and drove truck 6, they also show that truck 6 was idling at 402 Leon Pratt Drive, Wapakoneta, OH, in this district, from 09:51-10:17 UTC.

g. On December 5, 2024, at 13:13 and 13:14 UTC, TARGET ACCOUNT 1 sent ***two*** files to a group chat with multiple other users and did so using the same IP address and port. These files were uploaded using Verizon IP 174.219.212.255, port 1062. The images (file names f2859cee-7a26-4703-b727-a6ac3bdebfd0 and c3424da4-b4ba-44a8-8c42-b142f35542c2) depict a prepubescent child, lying down with her legs spread, with a focus on her vagina and anus but taken from different angles and with one zoomed in more. Verizon records show that SCHWERIN's phone **419-231-2471** used that IP, ports 1056-1087, from 09:53-20:08 UTC, meaning these files were uploaded from TARGET ACCOUNT 1 on a phone assigned SCHWERIN's number. Cached on his phone were GPS coordinates for the date/times of the file uploads and they came back to this District. Likewise, Buschur's records show that SCHWERIN was working that day, he was driving truck 6, and truck 6's GPS data showed it was not moving from 13:12-13:20 UTC and located at 402 Leon Pratt Drive in Wapakoneta.

51. KIK TARGET ACCOUNT 2, **taste.ur.vag.**, distributed to another user on October 25, 2024, at 15:24 UTC file name 3d798129-b549-477d-be7b-2d6ac4c2a167, a 43-second video depicting a prepubescent minor, naked from the waist down (other than an article of clothing around her waist), lying on her back with her legs spread and her knees positioned outward and up towards her head as an adult male penis repeatedly penetrates her vagina. This file was uploaded

using Verizon IP 174.196.96.179, port 62821, and Verizon records show that SCHWERIN's phone number **419-231-2471** used that IP, ports 62816-62847, from October 24, 2024 at 16:52 UTC, to October 29, 2024 at 13:07 UTC. Thus, these files were uploaded from TARGET ACCOUNT 2 on a phone that was assigned SCHWERIN's phone number.

h. Forensic examination of SCHWERIN's phone did not yield GPS coordinates at the exact date and time of the file upload but there were GPS coordinates for times in close proximity before and after the upload. At 14:38 UTC, 46 minutes before the file upload, the phone's GPS coordinates came back to Bellefontaine, Ohio in the Southern District of Ohio. At 15:46 UTC, 22 minutes after the file upload, the phone's GPS coordinates showed that it was at 402 Leon Pratt Drive in Wapakoneta in the Northern District of Ohio.

i. SCHWERIN's work schedule, as provided by Buschur, showed that he worked on October 25, 2024, and was in truck 35. Buschur's GPS data shows that truck 35 was moving and on State Route 65 in Wapakoneta.

j. Buschur's GPS data for truck 35's entire route on October 25, 2024, shows that truck 35 drove from Bellefontaine to Wapakoneta, consistent with SCHWERIN's phone being in Bellefontaine 46 minutes before the file upload.

52. Based on the above, Affiant submits that 13 CSAM files described herein were distributed by one of the KIK TARGET ACCOUNTS in this District and that 11 of the CSAM files were distributed on the Verizon Cellular network on a device with SCHWERIN's phone number **(419-231-2471)**. In addition, there were two CSAM files distributed from the home internet at SCHWERIN's residence, and his phone's GPS data showed that he was at his Wapakoneta residence when those files were distributed.

RELEVANT CONDUCT

53. [redacted]

54. [redacted]

55. [redacted]

56. [redacted]

57. [redacted]

58. [redacted].

a. [redacted]

b. [redacted]

c. [redacted]

CONCLUSION

59. Based on the foregoing, there is probable cause to believe SCHWERIN has violated 18 U.S.C. §§ 2252(a)(1), transportation of a visual depiction of a minor engaged in sexually explicit conduct; 2252(a)(2), receipt and distribution of visual depictions of minors engaged in sexually explicit conduct; and 2252(a)(4)(B), possession of visual depictions of minors engaged in sexually explicit conduct.

60. Accordingly, Affiant respectfully requests that the Court issue an arrest warrant for Seth Jacob SCHWERIN.

Respectfully submitted,

Anthony Safford
Special Agent
Homeland Security Investigations

Sworn to via telephone after submission by reliable electronic means on this 5th day of March, 2025. Fed. R. Crim. P. 4.1 and 41(d)(3).

DARRELL A. CLAY
UNITED STATES MAGISTRATE JUDGE